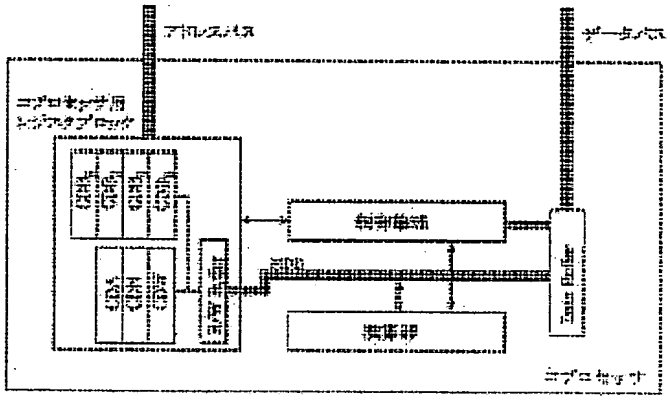
IC CARD AND MICROCOMPUTER

Publication number: JP2001195555 (A)
Publication date: 2001-07-19
Inventor(s): TERAUCHI CHIAKI; NAKADA KUNIHIKO; TSUKAMOTO TAKU; WATASE HIROSHI
Applicant(s): HITACHI LTD; HITACHI ULSI SYS CO LTD
Classification:
- international: ***G06F12/14; G06F21/24; G06K19/07; G09C1/00;*** **G06F12/14; G06F21/00; G06K19/07; G09C1/00;** (IPC1-7): G06K19/07; G06F12/14; G09C1/00
- European:
Application number: JP20000003297 20000112
Priority number(s): JP20000003297 20000112

Also published as:
JP4168305 (B2)

Abstract of **JP 2001195555 (A)**

PROBLEM TO BE SOLVED: To provide an IC card and a microcomputer, for which the strengthening of secrecy protection is realized. SOLUTION: Concerning the IC card or microcomputer in module configuration provided with the input/output operation of data accompanied with enciphering or deciphering processing by an arithmetic unit for cipher processing to be operated by supplying an operating voltage by electrically connecting an external terminal with a reader/writer and receiving an instruction from a central processing unit, the arithmetic unit for cipher processing is provided with a register for storing data to be used for operation for enciphering or deciphering processing for the unit of plural bits and before enciphering or deciphering processing, the required data are fetched into such a register.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－195555
（P2001－195555A）
(43)公開日　平成13年７月19日(2001.7.19)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　19/07		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　1/00	６２０Ｂ	５Ｂ０３５
Ｇ０９Ｃ　1/00	６２０		６５０Ａ	５Ｊ１０４
	６５０		６６０Ａ	９Ａ００１
	６６０	Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数13　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－3297(P2000－3297)

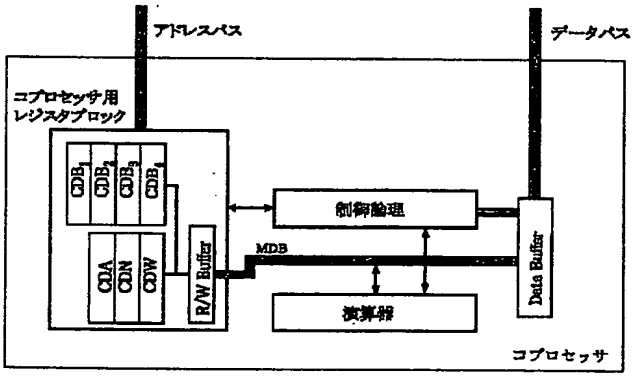
(22)出願日　平成12年１月12日(2000.1.12)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000233169
株式会社日立超エル・エス・アイ・システムズ
東京都小平市上水本町５丁目22番１号
(72)発明者　寺内　千晶
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(74)代理人　100081938
弁理士　徳若　光政

最終頁に続く

(54)【発明の名称】　ＩＣカードとマイクロコンピュータ

(57)【要約】
【課題】　機密保護の強化を実現したＩＣカードとマイクロコンピュータを提供する。
【解決手段】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカード又はモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかるレジスタに取り込むようにする。



1

【特許請求の範囲】

【請求項１】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードであって、

上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納してなることを特徴とするＩＣカード。

【請求項２】　請求項１において、

上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、

上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記レジスタから取り込むものであることを特徴とするＩＣカード。

【請求項３】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードであって、

上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を有することを特徴とするＩＣカード。

【請求項４】　請求項３において、

上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、

上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、かかる演算と並行して複数ビットの組み合わせに対応したＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むものであることを特徴とするＩＣカード。

【請求項５】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードであって、

上記中央処理装置は、暗号化又は復号化処理のためのデータが格納された先頭アドレスを上記記憶回路に供給し、上記記憶回路は上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出されるものであることを特徴とするＩＣカード。

【請求項６】　請求項５において、

上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、

上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、上記複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むものであることを特徴とするＩＣカード。

【請求項７】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードであって、

上記中央処理装置は、上記乱数発生回路で形成された乱数を用いて形成された暗号化されたアドレス信号を上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成し、

上記記憶回路は、上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいて暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、

かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには上記乱数発生回路で形成された乱数が偽アドレス信号として送出されるものであることを特徴とするＩＣカード。

【請求項８】　請求項７において、

上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、

上記暗号処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、上記複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むものである

ことを特徴とするＩＣカード。

【請求項９】　中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納してなることを特徴とするマイクロコンピュータ。

【請求項１０】　請求項９において、

上記モジュール構成は、１つの半導体基板上において形成されることによって実現されることを特徴とするマイクロコンピュータ。

【請求項１１】　中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を有することを特徴とするマイクロコンピュータ。

【請求項１２】　中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記中央処理装置は、暗号化又は復号化処理のためのデータが格納された先頭アドレスを上記記憶回路に供給し、

上記記憶回路は上記先頭アドレスを基に内蔵されたアドレス発生回路により形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットにデータ転送し、

上記乱数発生回路は、上記データ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに生成した乱数を偽アドレス信号として送出することを特徴とするマイクロコンピュータ。

【請求項１３】　中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータであって、

上記中央処理装置は、上記乱数発生回路で形成された乱数を用いて形成された暗号化されたアドレス信号を上記記憶回路に供給し、

上記記憶回路は、上記中央処理装置から供給された上記暗号化されたアドレス信号を上記乱数を用いて復号化して先頭アドレスを生成し、暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、

上記乱数発生回路は、上記データ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに生成した乱数を偽アドレス信号として送出することを特徴とするマイクロコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＩＣカードとマイクロコンピュータに関し、特にＩＣカードやプログラム内蔵の１チップマイクロコンピュータのようなＣＰＵとメモリを含み暗号鍵を使ったデータ処理を行なうものの機密保護技術に利用して有効な技術に関するものである。

【０００２】

【従来の技術】メモリに保存されている鍵情報を用いてデータの暗号化処理又は復号化処理を行なうようにしたＩＣカードにおいて、処理時間の違いを利用して実行内容や暗号鍵を推定するＴＡ（Timing Attack）法のようなハッキング手法に対抗するため、暗号処理化又は復号化処理の実行中又は実行の前後に、鍵情報の内容との時間的な相関関係を喪失させる遅延処理を実行する技術の例として、特開平１０－６９２２２号がある。また、ＩＣカードに関しては、オーム社出版電子情報通信学会編水沢順一著「ＩＣカード」などがある。

【０００３】

【発明が解決しようとする課題】近年、ＩＣカードが暗号処理を行っている時の消費電流を観測して解析することにより、容易に暗号処理の内容や暗号鍵が推定されることの可能性が示唆されている。このことについては、John Wiley & sons 社 W.Rankl & W. Effing著「Smart Card Handbook」の8.5.1.1 Passive protective mechanisms(263ページ) に記載されている。

【０００４】つまり、ＳＰＡ（Simple Power Analysis）法では、演算命令の違い、あるいは処理されているデータの違いにより生じる消費電流波形の違いから、暗号鍵や処理されているデータを解析し、ＤＰＡ（Diffrential Power Analysis）法では、消費電流波形を統計処理して暗号鍵を推定する。このＤＰＡ法では、例えばＤＥＳのある部分に仮定した暗号鍵をあてはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

【０００５】前記公報に記載のようにＴＡ（Timing Attack）法のみを考慮した遅延処理では、実際の演算による消費電流の相関性までも喪失させることができず、上記のような消費電流波形を観測するというＳＰＡ又はＤ

ＰＡ法のようなハッキング手法には対抗できない。そこで、本願発明者等においては、上記ＩＣカード及びＩＣカード等のようなモジュールに搭載されるマイクロコンピュータのように内蔵のプログラムにより一定のデータ処理動作を行うものに対して上記のような消費電流の観測による暗号処理の内容や暗号鍵の解読をより確実に防止することができる機密保護技術を開発するに至った。

【０００６】この発明の目的は、機密保護の強化を実現したＩＣカードとマイクロコンピュータを提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【０００７】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかるレジスタに取り込むようにする。

【０００８】本願において開示される発明のうち他の代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに取り込むようにする。

【０００９】

【発明の実施の形態】図１には、この発明が適用されるＩＣカードの一実施例の外観図が示されている。ＩＣカードは、プラスチックケースからなるカード１０１と、かかるカード１０１の内部に搭載された図示しない１チップのマイクロコンピュータ等からなるＩＣカード用チップを持つものである。上記ＩＣカードは、さらに上記ＩＣカード用チップの外部端子に接続されている複数の接点（電極）１０２を持つ。複数の接点１０２は、後で図２によって説明するような電源端子ＶＣＣ、電源基準電位端子ＶＳＳ、リセット入力端子ＲＥＳバー、クロック端子ＣＬＫ、データ端子Ｉ／Ｏ－１／ＩＲＱバー、Ｉ／Ｏ－２／ＩＲＱバーとされる。ＩＣカードは、かかる接点１０２を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部結合装置との間でのデータの通信を行う。

【００１０】図２には、この発明に係るＩＣカードに搭載されるＩＣカード用チップ（マイクロコンピュータ）の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知のＭＯＳ集積回路の製造技術により、特に制限されないが、単結晶シリコンのような１個の半導体基板上において形成される。

【００１１】この発明に係るＩＣカード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路２０５、中央処理装置（以下単にＣＰＵという場合がある）２０１、ＲＯＭ(Read Only Memory)２０６やＲＡＭ(Random Access Memory)２０７、不揮発性メモリ２０８などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ２０９、入出力ポート（Ｉ／Ｏポート）２０２などからなる。

【００１２】クロック生成回路２０５は、図示しないリーダライタ（外部結合装置）から図１の接点１０２を介して供給される外部クロックＣＬＫを受け、かかる外部クロック信号に同期したシステムクロック信号を形成し、それをチップ内部に供給する回路である。ＣＰＵ２０１は、論理演算や算術演算などを行う装置であり、システムコントロールロジック、乱数発生器及びセキュリィロジック及びタイマなどを制御する。記憶装置２０６、２０７、２０８は、プログラムやデータを格納する装置である。コプロセッサ２０９は、後述するようにＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を行なう演算器とレジスタ及び制御論理から構成される。Ｉ／Ｏ（入出力）ポート２０２は、リーダライタと通信を行う装置である。データバス２０４とアドレスバス２０３は、各装置を相互に接続するバスである。

【００１３】上記記憶装置２０６，２０７，２０８のうち、ＲＯＭ２０６は、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ（以下、ＲＡＭという）２０７は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ＩＣカードがリーダライタから抜かれると電源の供給が中断されるため、ＲＡＭ２０７の内容は、保持されなくなる。

【００１４】上記不揮発性メモリ（以下、ＥＥＰＲＯＭ(Electrical Erasable Programmable Read Only Memory)という）２０８は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このＥＥＰＲＯＭ２０８は、書き換える必要があり、かつＩＣカードがリーダライタから抜かれても保持すべきデータを格納するために使われる。例えば、ＩＣカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この

場合の度数などは、リーダライタか抜かれてもＩＣカード内で記憶保持する必要があるため、ＥＥＰＲＯＭ２０８で保持される。

【００１５】ＣＰＵ２０１は、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令ＲＯＭ、演算回路、汎用レジスタ（ＲＧ６等）、内部バスＢＵＳに結合するバスドライバ、バスレシーバなどの入出力回路を持つ。ＣＰＵ２０１は、ＲＯＭ２０６などに格納されている命令を読み出し、その命令に対応する動作を行う。ＣＰＵ２０１は、Ｉ／Ｏポート２０２を介して入力される外部データの取り込み、ＲＯＭ２０６からの命令や命令実行のために必要となる固定データのようなデータの読み出し、ＲＡＭ２０７やＥＥＰＲＯＭ２０８に対するデータの書き込みと読み出し動作制御等を行う。

【００１６】上記ＣＰＵ２０１は、クロック生成回路２０５から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。ＣＰＵ２０１は、その内部の主要部がＰチャンネル型ＭＯＳＦＥＴとＮチャンネル型ＭＯＳＦＥＴとからなるＣＭＯＳ回路から構成される。特に制限されないが、ＣＰＵ２０１は、ＣＭＯＳスタティックフリップフロップのようなスタティック動作可能なＣＭＯＳスタテック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うようなＣＭＯＳダイナミック回路とを含む。

【００１７】ＩＣカードのセキュリティ機能としては、チップ内部で乱数を自動生成する乱数発生器や、ランダムに割込みを生成するタイマー機能などの他に、本願発明にかかる高セキュリテイ機能として、ＩＣカードと外部装置とのデータ送受信の際に用いるＲＳＡ暗号法などに応用可能なべき乗剰余演算動作を行なう暗号処理用演算ユニット（コプロセッサ）２０９を内蔵している。このコプロセッサ２０９は専用のレジスタが内蔵されている。

【００１８】ＩＣカードにおけるセキュリティ・システムでは、通信データの暗号処理は必須であり、この実施例でも現在最も多く利用されている公開鍵暗号としてＲＳＡ暗号が用いられる。この暗号法では、暗号化・復号化ともにべき乗剰余乗算X^Y ｍｏｄＮを用いるが、これは公知のMontgomry法といわれる計算アルゴリズムによって剰余乗算A^2 ｍｏｄＮとＡＢｍｏｄＮの２つの形に分解することができる。つまり、Ｙ＝e_n e_{n-1} ・・・ e_1 の値e_i を上位e_n から最下位のe_1 まで順に１ビットずつ見ていき、e_i ＝０だったらA^2 ｍｏｄＮのみを、e_i ＝１だったらA^2 ｍｏｄＮとＡＢｍｏｄＮを演算する。したがって、e_i ＝０のときにはA^2 ｍｏｄＮの演算の後にｉ＝０であるかの判定処理が行なわれ、e_i ＝１のときにはA^2 ｍｏｄＮとＡＢｍｏｄＮとの演算の後にｉ＝０であるかの判定処理が行なわれるために、e_i ＝０と１とに対応した２通りの電流波形の形態が現れてしまう。

【００１９】この実施例のようにコプロセツサ２０９を用いた場合には、その消費電流はＣＰＵの消費電流に比べて比較的大きいため、この部分の電流波形を観測することによりコプロセッサの動作形態を比較的容易に識別することができ、前記ＴＡ法とＳＰＡ法により暗号鍵Ｙの値をハッキングされてしまう可能性が高い。そこで、この実施例のコプロセッサ２０９では、上記暗号化・復号化ともに用いられるべき乗剰余乗算X^Y ｍｏｄＮの演算を行なうに当たり攪乱目的のダミーの演算が挿入される。つまり、図３のタイミング図及び図４のフローチャート図に示すようにe_i ＝０でも１でもA^2 ｍｏｄＮとＡＢｍｏｄＮの両方の演算を常に行なうようにするものである。

【００２０】図３のタイミング図において、（ａ）に示すように本来は、e_n ＝１のときにはA^2 ｍｏｄＮの演算を行い、e_n の判定の１により時間ｔ１を経てＡＢｍｏｄＮの演算を行い、その演算後にｉをデクリメント（ｎ－１）してｉ＝０の判定に時間ｔ２を費やす。次いで、次ビットe_{n-1} ＝０のときは、A^2 ｍｏｄＮの演算を行い、e_{n-1} ＝０の判定とｉをデクリメント（ｎ－２）してｉ＝０の判定に時間ｔ３を費やす。そして、次ビットe_{n-2} ＝１のときには、A^2 ｍｏｄＮの演算を行い、e_{n-2} の判定の１により時間ｔ１を経てＡＢｍｏｄＮの演算を行い、その演算後にｉをデクリメント（ｎ－３）してｉ＝０の判定に時間ｔ２を費やす。以下、同様にe_1 まで同様な動作を繰り返すものである。

【００２１】この実施例のコプロサッサ２０９においては、上記暗号鍵Ｙの各ビットe_i の論理０又は１に無関係にA^2 ｍｏｄＮの演算の後にＡＢｍｏｄＮの演算を行なうようにする。図３（ｂ）のe_{n-1} ＝０のときのようにe_i が論理０のときにおける上記ＡＢｍｏｄＮの演算が攪乱目的のダミー演算として挿入される。つまり、（ｂ）のタイミング図及び図４のフローチャート図のように、A^2 ｍｏｄＮとＡＢｍｏｄＮの演算動作の間には、例えばe_i の判定の判定を含む時間ｔ１が費やされ、ＡＢｍｏｄＮと次ビットに対応したA^2 ｍｏｄＮの演算動作の間には、ｉのデクリメント動作とｉ＝０の判定時間ｔ２が費やされる画一化された動作タイミング及び動作電流とすることができる。ただし、この実施例では、e_i の判定処理は、その結果が演算動作の分岐の条件とされないため図４のフローチャート図では省略されている。

【００２２】図５には、上記コプロセッサの一実施例のブロック図が示されいてる。この実施例では、主に演算器、制御論理、専用レジスタブロックより構成され、べ

き乗剰余演算の最終結果はデータバツファ、データバスを介して中央処理装置ＣＰＵに送信される。専用レジスタは、アドレスバスから供給されるアドレス信号に対応してその選択動作が行なわれる。

【００２３】この実施例では、内部バスＭＤＢとレジスタブロックのリードライトバッファ（Ｒ／Ｗ　Buffer）との間にゲート回路１が設けられる。このゲート回路１は、制御論理により制御が行なわれて、e_i が論理０ならばA^2 ｍｏｄＮ動作の演算結果が内部バスＭＤＢとリードライトバッファを介して所定のレジスタＣＤＡに取り込まれた後開いていたゲートが閉じるようにされる。つまり、上記演算結果がリードライトバッファに取り込まれると、その後にゲートを閉じてしまいリードライトバッファへの新たなデータの書き込みを禁止する。したがって、その後に行なわれるＡＢｍｏｄＮの演算結果は無効データとして扱われることとなる。また、e_i が論理１ならばゲート回路１はゲートを開いた状態のままとされる。

【００２４】図６には、上記コプロセッサの他の一実施例のブロック図が示されている。この実施例では、レジスタブロックのリードライトバッファ（Ｒ／Ｗ　Buffer)と各レジスタとの間にゲート回路２が設けられる。このゲート回路２は、前記同様に制御論理により制御が行なわれて、e_i が論理０ならばA^2 ｍｏｄＮ動作の演算結果が内部バスＭＤＢとリードライトバッファとを介して所定のレジスタＣＤＡに書き込まれた後に開いていたゲートが閉じるようにされる。つまり、上記演算結果がレジスタＣＤＡに取り込まれると、その後にゲートを閉じてしまいかかかるレジスタＣＤＡへの新たなデータの書き込みを禁止する。したがって、その後に行なわれるＡＢｍｏｄＮの演算結果は、リードライトバッファまでは書き込まれるが、実際には無効データとして扱われることとなる。また、e_i が論理１ならばゲート回路２はゲートを開いた状態のままとされる。

【００２５】図７には、上記ゲート回路の一実施例の内部構成図が示されている。ダミー書き込み制御ユニットは、アンドゲート回路によって構成され、一方の入力には制御論理からのライトイネーブル信号が供給され、他方の入力には演算器で生成されたライトストローブ信号が供給される。上記ゲート回路の出力信号は、データバッファ（Ｒ／Ｗ　Buffer)と専用レジスタにライトストローブ信号として伝えられる。

【００２６】この実施例では、演算結果そのものの伝達制御するものに代えて、レジスタ又はデータバッファへの書き込み動作を指示するライトストローブ信号の発生タイミングを切り換えるようにするものである。つまり、e_i ＝０のときには、A^2 ｍｏｄＮ動作の演算結果が出力された後にライトイネーブル信号をロウレベルとしてアンドゲート回路のゲートが閉じるようにするものである。逆に、e_i ＝１のときには、制御論理はライトイネーブル信号をハイレベルのままとして、演算器で形成されたライトストローブ信号がそのままデータバッファ又は専用レジスタに伝えられる。この構成では、複数ビットからなる演算結果Ａに対応して、複数個のゲート回路を設ける必要がないので簡素化が可能になる。

【００２７】図８には、上記コプロセッサの他の一実施例のブロック図が示されいてる。この実施例では、レジスタブロックのリードライトバッファ（Ｒ／Ｗ　Buffer)と各レジスタとの間にセレクタ２とレジスタブロックにダミーレジスタ１が設けられる。このセレクタ２は、前記同様に制御論理により制御が行なわれて、e_i が論理０ならばA^2 ｍｏｄＮ動作の演算結果が内部バスＭＤＢとリードライトバッファとを介して所定のレジスタＣＤＡに書き込まれるような信号経路を形成し、その後にダミーレジスタ１を選択するような信号経路を形成する。

【００２８】つまり、上記演算結果がレジスタＣＤＡに取り込まれると、その後にダミーレジスタ１を選択するので、レジスタＣＤＡへの新たなデータの書き込みを禁止しつつその後に行なわれるＡＢｍｏｄＮの演算結果がダミーレジスタに書き込まれものとなる。e_i が論理１ならばセレクタ２は常にレジスタＣＤＡを選択する。この構成は、演算結果をレジスタに書き込む動作を含めてe_i が論理０のときと論理１のときとで電流波形でみたときに全く同一にすることができるから、電流波形を利用したアタックをより確実に無力化することができる。

【００２９】図９には、この発明に係るコプロセッサの他の一実施例の動作を説明するための構成図が示されている。図９（ａ）のタイミング図及び（ｂ）のフローチャート図において、前記説明したように、A^2 ｍｏｄＮの演算後、e_i の判定の時間ｔ１の間もダミー演算動作としてA^2 ｍｏｄＮを継続してＡＢｍｏｄＮの演算に移行する。

【００３０】その演算後にｉをデクリメント（－１）してｉ＝０の判定に時間ｔ２を費やすが、その間も上記ＡＢｍｏｄＮの演算を継続させる。以下、同様にe_i まで同様な動作を繰り返すものである。この構成は、演算動作中は、e_i が論理０と１のときに関係なく上記のような演算動作を継続するので、電流波形でみたときに格別な特徴を見出すことができないから、電流波形を利用したアタックを無力化することができる。

【００３１】図１０には、図９のコプロセッサの動作を実現するための一実施例のブロック図が示されている。制御論理では、ダミーイネーブル信号とコプロイネーブル信号を送出する。上記ダミーイネーブル信号とコプロイネーブル信号は、オアゲート回路を通して演算器に入力される。それ故、コプロイネーブル信号がアクティブであるときに加えて、ダミーイネーブル信号がアクティブであるときにも演算器は演算動作を行なうようにされる。

【００３２】上記ダミーイネーブル信号は、インバータ回路を通してアンドゲート回路の一方の入力に供給され、かかるアンドゲート回路の他方の入力には演算器で形成されたライトストローブ信号が供給される。つまり、演算器で形成されたライトストローブ信号の伝達をダミーイネーブル信号で選択的に停止できるようにする。コプロイネーブル信号がアクティブにされて、前記正規の演算動作が終了すると、その演算結果を出力するためのライトストローブ信号が形成される。このようにコプロイネーブル信号がアクティブのときには、ダミーイネーブル信号の反転信号がアクティブレベルとなってアンドゲート回路のゲートを開くように制御するので、上記正規演算結果はライトストローブ信号によって、Ｒ／Ｗバッファ又はレジスタブロックの所定のレジスタに書き込まれる。

【００３３】上記のような正規演算が終了すると、ダミーイネーブル信号がアクティブとなって演算器に対して演算動作を指示する。この演算の終了によって、上記ライトストローブ信号が形成されるが、上記ダミーイネーブル信号の反転信号によってアンドゲート回路がゲートを閉じているので、上記撹乱目的のダミー演算動作によって発生されたライトストローブ信号がＲ／Ｗバッファ又はレジスタブロックの所定のレジスタに伝えられることはない。これにより、撹乱目的のダミー演算結果は無効データとして消失させられる。

【００３４】図１１には、この発明に係るコプロセッサの他の一実施例の動作を説明するためのタイミング図が示されている。前記図３に示した実施例のように、撹乱目的のダミー演算を挿入して、（ａ）のタイミング図のように、e_i に対して画一化してA^2 ｍｏｄＮとＡＢｍｏｄＮの演算を一対として行なうようにした場合でも、各演算には、演算結果にオーバーフロー処理を必要とするもの（あり）のものと、オーバーフロー処理を必要としないもの（なし）が発生する。

【００３５】このようなオーバーフロー処理は、演算時間を長くするものであるので電流波形でみると、オーバーフロー処理ありとなしとの識別が可能になる。このような電流波形の特徴から演算内容や演算データを推測することも不可能ではないと考えられるため、この実施例では（ｂ）のタイミング図に示すようにオーバーフロー処理を不要とする演算に対しても必要なときと同様にオーバーフロー処理を挿入する。つまり、みかけ上は、全ての演算A^2 ｍｏｄＮとＡＢｍｏｄＮの演算において画一的にオーバーフロー処理のための動作が実施されるために、その識別を無力化するものである。

【００３６】図１２は、この発明に係るコプロセッサの他の一実施例の動作を説明するためのフローチャート図が示されている。このフローチャート図は、前記図１１（ｂ）に対応している。A^2 ｍｏｄＮとＡＢｍｏｄＮの各演算は、剰余演算部とオーバーフロー演算部からなり、演算結果に無関係に上記オーバーフロー演算処理を実施するものである。

【００３７】図１３には、この発明に係るコプロセッサの他の一実施例の動作の詳細を説明するためのタイミング図が示されている。この実施例による対策前では、前記A^2 ｍｏｄＮとＡＢｍｏｄＮのようなコプロ演算においては、その演算結果に対応してオーバーフロー処理のあるものと無いもの２種類が存在したが、この実施例による対策後では、前記A^2 ｍｏｄＮとＡＢｍｏｄＮのようなコプロ演算においては、その演算結果に無関係に常にオーバーフロー処理が実行される。このため、本来はオーバーフロー処理が不要な演算動作に対して実施されたオーバーフロー処理は、撹乱目的のダミー動作とされる。

【００３８】図１４には、図１１ないし図１３に示したコプロセッサの動作を実現するための一実施例のブロック図が示されている。制御論理では、ダミーオーバーフロー信号とコプロオーバーフロー信号を送出する。上記ダミーオーバーフロー信号とコプロオーバーフロー信号は、オアゲート回路を通して演算器に入力される。それ故、コプロオーバーフロー信号がアクティブであるときに加えて、ダミーオーバーフロー信号がアクティブであるときにも演算器はオーバーフロー処理動作を行なうようにされる。

【００３９】上記コプロオーバーフロー信号は、アンドゲート回路の一方の入力に供給され、かかるアンドゲート回路の他方の入力に演算器で形成されたライトストローブ信号が供給される。つまり、演算器で形成されたライトストローブ信号の伝達をコプロオーバーフロー信号がアクティブレベルでないときに選択的に停止できるようにする。つまり、コプロオーバーフロー信号がアクティブレベルでないときはダミーオーバーフロー信号によって演算器がオーバーフロー処理を行なっているので、かかるオーバーフロー処理で形成されたライトストローブ信号は上記ゲート回路のゲートを閉じることによって無効にするものである。したがって、前記正規のオーバーフロー処理終了すると、その処理結果を出力するためのライトストローブ信号が形成されて、Ｒ／Ｗバッファ又はレジスタブロックの所定のレジスタに処理結果が書き込まれる。

【００４０】これに対して、ダミーオーバーフロー信号がアクティブとなって演算器に対してオーバーフロー処理動作を指示した場合には、そのオーバーフロー処理によって形成されたライトストローブ信号は、上記コプロオーバーフロー信号によってアンドゲート回路のゲートが閉じられるものであるから、上記撹乱目的のダミーオーバーフロー処理動作によって発生されたライトストローブ信号がＲ／Ｗバッファ又はレジスタブロックの所定のレジスタに伝えられることはない。これにより、撹乱目的のダミーオーバーフロー処理結果は無効データとし

て消失させられる。

【００４１】図１５には、この発明に係るコプロセッサの更に他の一実施例の動作を説明するためのタイミング図が示されている。（ａ）に示すように本来は、e_n＝１のときにはA^2 ｍｏｄＮの演算を行い、e_nの判定の１により時間ｔ１を経てＡＢｍｏｄＮの演算を行い、その演算後にｉをデクリメント（ｎ－１）してｉ＝０の判定に時間ｔ２を費やす。次いで、次ビットe_{n-1}＝０のときは、A^2 ｍｏｄＮの演算を行い、e_{n-1}＝０の判定とｉをデクリメント（ｎ－２）してｉ＝０の判定に時間ｔ３を費やすような演算動作に対して、上記各演算毎の時間ｔ１、ｔ２及びｔ３に対して攪乱目的のダミーサイクルが挿入される。

【００４２】（ｂ）のタイミング図では、上記攪乱目的のダミーサイクルの挿入は、各演算毎の時間を最も長い時間ｔ３に揃えるように挿入するものである。これにより、時間ｔ３をインターバルとしてA^2 ｍｏｄＮ又はＡＢｍｏｄＮのいずれかの演算が実施されるために、みかけ上は演算動作に対応した電流波形が画一化されてその識別を無力化するものである。これに対して、（ｃ）タイミング図では、上記（ｂ）とは逆に上記演算毎のインターバルにおいて時間がランダムに変化する攪乱目的のダミーサイクルが挿入される。上記A^2 ｍｏｄＮ又はＡＢｍｏｄＮのいずれかの演算が時間的にランダムに実施される。そのため、電流波形でみると上記各演算動作と無関係で、かつ不規則性の電流値にされる。言い換えるならば、上記演算器において同じ状態及び同じ動作でも毎回異なるよう、統計的な観点での非再現性を持つようにされるために、その識別を無力化することができる。

【００４３】上記のような攪乱目的のダミーサイクルは、前記図２に示されたようにタイマーを利用して演算間隔を可変にするものである。あるいはコプロセッサの外部にタイマーを設けて一定の時間が経過するまで次の演算の実行を待つようにする。つまり、コプロセッサによるべき乗剰余乗算の演算において、図１５（ａ）に示した前記各演算毎の時間ｔ１，ｔ２，ｔ３に攪乱目的のダミーのサイクルを挿入し、一定時間後にタイマーからの割込みを入れる。これにより、図１５（ｂ）に示すようにｔ１，ｔ２，ｔ３の時間が全て一定となり、電流波形からのアタックを困難にする。あるいはタイマーには乱数発生器で生成した乱数をセットしておき、（ｃ）に示すように毎回ｔ１，ｔ２，ｔ３の時間をランダムに変化させることも可能である。また、タイマーを用いなくても、ソフトウエアでカウントすることも可能である。

【００４４】べき乗剰余乗算において、コプロセッサによる演算の高速化を目的とし、Ｙの値を２ビット、あるいは３ビットずつ処理するようにすると、例えば図１６のフローチャート図に示すように、２ビット処理の例で説明するなら常にA^2 ｍｏｄＮ－A^2 ｍｏｄＮ－ＡＢｍｏｄＮ及びｉ－２とｉ＝０？の各ステップの繰り返しになるので、前記１ビットずつ行なう場合のような攪乱目的のダミー演算を行なわなくとも、処理時間や電流波形が一定になる。そのため、電流波形からＹの値を推定するのは困難になる。また演算の回数も、前記のバイナリ法だと最大で２ｎ回かかっていたものを、２ビット処理だと常に１．５ｎ回で済むために、動作時間の短縮にもつながる。

【００４５】コプロセッサの演算が開始するまでにＡ，Ｂ，Ｎの値をそれぞれコプロセツサ専用レジスタに転送し格納しておく。しかしながら、２ビット処理を行う場合、、Ｙの値によって４通りのＢの値B_1、B_2、B_3、B_4が必要になり、これらの値は前もって計算して．ＲＡＭやＥＥＰＲＯＭなどに格納しておきヽ毎回コプロセツサ専用レジスタに転送することになるが。この際、４通りのＢの値によって転送中の電流波形に特徴が現れる可能性がある。

【００４６】例えば、１６ビットのプリチャージバスにデータを転送する場合を考える。プリチャージバスは、データ転送の前にすべてのバスの値を“１”にそろえるバスである。このバスに、値は違うが“１”のビットの数が同じデータ、例えば、“１”のビットの数が２である１６進数で“８８”と“１１”、を転送した場合、電流波形はほぼ同じ波形になると予測される。この理由は、“１”から“０”へ変化したビットの数が同じであるため、同じように電流を消費し、同じ電流波形になるからである。

【００４７】もし、“１”のビットの数が１つ異なるデータ、例えば、“１”のビットの数が３である“８９”や“１９”を転送した場合、“１”のビットの数が２のデータとは消費電流が異なる。これは、１３ビット分バスの値が“１”から“０”に変わったため、その分の電流が消費される。そのため、先の１４ビットが変化したデータに比べて消費電流が１ビット分小さくなる。一般に、変化するビットの数が多いほど電流波形は高くなるという規則性がある。この規則性から転送されているデータを推定することができると思われる、電流アタックの対象となりやすい。これを防ぐため次のような工夫を行なうものである。

【００４８】図１７と図１８には、この発明に係るコプロセッサの他の一実施例のブロック図がそれぞれ示されている。この実施例のコプロセッサは、２ビット処理と３ビット処理に向けられている。つまり、コプロセッサのレジスタ容量を増やして、２ビット処理の場合には４通りのＢの値B_1～B_4を、３ビット処理の場合には８通りのＢの値B_1～B_8をコプロセッサのレジスタに格納しておく。従って、演算の途中で記憶回路（ＲＡＭ）からデータバスを通して上記コプロセッサのれレジスタに前記のような転送の必要がなくなり、前記電流アタックに対して防御することができる。

【００４９】つまり、前記図１６に示したようなフロー

チャート図において、コプロセッサがＡＢｍｏｄＮを実行する際、下記のように４つ（３ビット処理のときにはあるいは８つ）のうちの正しいＢレジスタＣＤＢから値を選んで実行できるように、Ｙの２ビット（あるいは３ビット）の値をコプロセッサの制御レジスタ（ＣＣＮ＊Ｔ）のビットに当てはめ、次に示す制御レジスタ及び演算の種類のように、２ビット処理の場合には、AB_1 ｍｏｄＮ，AB_2 ｍｏｄＮ，AB_3 ｍｏｄＮ，AB_4 ｍｏｄＮのうちどの演算をするかを選択させるようにする。

【００５０】

制御用レジスタ（ＣＣＮＴ）

ビット７	ビット６	.....	ビット２	ビット１	ビット０
－	－			e_1	e_{1-1}

【００５１】

演算の種類

ビット２	e_1	e_{1-1}	演算の種類
0	0	0	$A \leftarrow A^2$ ｍｏｄＮ
0	1	0	$A \leftarrow A$ ｍｏｄＮ
0	1	1	$A \leftarrow A \times N$
1	0	0	$A \leftarrow AB_1$ ｍｏｄＮ
1	0	1	$A \leftarrow AB_2$ ｍｏｄＮ
1	1	0	$A \leftarrow AB_3$ ｍｏｄＮ
1	1	1	$A \leftarrow AB_4$ ｍｏｄＮ

【００５２】図１９には、この発明に係るコプロセッサの他の一実施例のブロック図が示されている。この実施例のコプロセッサも、２ビット処理や３ビット処理のような複数ビット処理に向けられている。この実施例では、データバスにスイッチを設けて演算をしながら転送できるようにする。この構成により、コプロセッサのレジスタ容量を増加させることなく、実行時間の短縮と電流アタック対策の両方に効果的である。

【００５３】コプロセツサ専用レジスタ（ＣＤＡ，ＣＤＢ，ＣＤＮ，ＣＤＷ）は、同図に示すように４つのレジスタがＣＰＵとコプロセッサの演算器との間で排他的に使用されている。２ビット処理を行う場合、２回のA^2 ｍｏｄＮを行いながらその間にＢの値をＲＡＭからコプロセッサ専用レジスタユニット中のＢレジスタＣＤＢに転送できるようにすると効率的である。

【００５４】コプロセッサのＡレジスタＣＤＡとＢレジスタＣＤＢのＩ／Ｏを分け、それぞれにリード／ライトバッファ（Ｒ／Ｗ　Buffer)を設けて、それぞれ独立に動作できるようにする。演算器がA^2 ｍｏｄＮを演算している間は、制御信号によりデータバスをパス１（ｐａｔｈ１）につなぎ、図示しないＣＰＵのＲＡＭからＢの値を上記独立に設けられたリード／ライトバッファを介してＢレジスタＣＤＢに転送する。次に演算器がＡＢｍｏｄＮを実行する際には、制御信号によりパス２（ｐａｔｈ２）に切り換え、上記Ｂレジスタの Ｂ値を演算器に送り上記ＣＰＵがＢレジスタＣＤＢにアクセスできないようにする。この方法を取ると、A^2 ｍｏｄＮを演算動作と、Ｂ値の転送動作が同時に行なわれるから演算時間が短縮されるだけでなく、演算と転送の消費電流が重なるため双方の波形が識別できなくなり、電流アタック対策に有効である。

【００５５】図２０には、この発明に係るＩＣカード用チップの他の一実施例の要部ブロック図が示されている。この実施例では、暗号処理用演算ユニットとメモリ（ＲＡＭ）間の転送の際、メモリにカウンタを設けるようにするものである。この実施例では、２ビット処理に用いる４通りの値、あるいは３ビット処理に用いる８通りの値をコプロセッサ外部メモリＲＡＭからコプロセッサ専用レジスタユニット中のＢレジスタＣＤＢに転送する際の電流撹乱を行なうようにするものである。

【００５６】この実施例では、前記図２に示したようなＩＣカード用チップにおいて、ＲＡＭの側にカウンタが設けられる。ＲＡＭは、カウンタで形成されたアドレス信号をデコードしてデータをデータバスに送出する。このとき、アドレスバスには、乱数発生器が形成された偽アドレスが送出される。これにより、アドレスとデータとの相関が無くなり、電流解析を無力化させることができる。

【００５７】図２１には、上記カウンタの一実施例のブロック図が示されている。カンウタは、転送したいブロックの最初のアドレスを保持する先頭アドレスレジスタとインクリメンタを用い、ブロック転送をイネーブルにするイネーブル信号とクロック又はリード／ライト信号などによるインクリメント指示信号で制御する。ブロッ

ク転送を開始する際、まず転送の先頭アドレスと転送開始のイネーブル信号がＣＰＵよりカウンタに送信され、上記先頭アドレスレジスタに保持される。その後は、インクリメント指示信号によって、インクリメンタが動作して先頭アドレスレジスタの先頭アドレスＡ＋１を形成して、アドレスを生成するとともに上記先頭アドレスレジスタの内容を書き換えるので、図２２のタイミング図に示すように、ＲＡＭアドレスが順番にインクリメントＡ、Ａ＋１、Ａ＋２、・・・されていき、そのアドレスに従って順次データD_A、D_{A+1}、D_{A+2}・・・・が書込まれ／読み出される。

【００５８】この実施例では、ブロック転送がイネーブルになった後はアドレスバスからのアドレスをカウンタが受け付けないため、アドレスバスにどのような値が来ようとデータは正しく読み出されていく。従って、アドレスバスに乱数発生器などで生成した乱数Ｂ、Ｃ、Ｄ、Ｅ・・・が出力されるとアドレスバスの消費電流を撹乱でき、この効果からチップ全体の消費電流を撹乱できるため、チップ内部動作の解析を困難にすることが可能になる。

【００５９】図２３には、この発明に係るＩＣカード用チップの更に他の一実施例を示す要部ブロック図が示されている。この実施例でも、暗号処理用演算ユニットとメモリ（ＲＡＭ）間の転送の際、メモリにカウンタを設けるようにするものであが、かかる暗号処理用演算ユニットとメモリＲＡＭの最初のアドレスをも撹乱するようアドレスオフセット機能が設けられる。つまり、乱数発生器などで生成した乱数をあらかじめＣＰＵとカウンタ側に同時に転送しておき、ブロック転送の最初のアドレスに乱数を加えるか又は引くかした値をアドレスバスに出力する。カウンタ側ではアドレスバスの値を同じ乱数を用いて復号化し、最初のアドレスを得る。

【００６０】図２４には、上記転送動作を説明するためのタイミング図が示されている。乱数発生器で形成された乱数をあらかじめＣＰＵとＲＡＭに転送しておき、オフセット演算部１によりブロック転送の最初のアドレスＡに乱数Ｓを加えるか引くかしたアドレスＡ±Ｓをアドレスバスに送出する。カウンタ側では、アドレスバスの値を同じ乱数Ｓを用いて復号化し、オフセット演算部２により最初のアドレスＡを得て、以後前記同様にインクリメントしてアドレスＡ＋１、Ａ＋２・・・を生成する。このようなアドレスＡ＋１、Ａ＋２に同期して、乱数発生器が乱数Ｂ、Ｃ、Ｄ・・・をアドレスバスに送出するので、先頭のアドレスを含めてアドレスバスの消費電流を撹乱でき、チップ内部動作の解析をいっそう困難にすることが可能になる。

【００６１】上記の実施例から得られる作用効果は、下記の通りである。すなわち、

（１）　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかるレジスタに取り込むようにすることにより、演算動作の過程でのデータ転送を無くすことができるから、電流波形でのハッキングを無力化することができるという効果が得られる。

【００６２】（２）　上記に加えて、上記暗号化処理又は復号化処理を、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含むものとし、上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2\ mod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2$ ｍｏｄＮの演算を行ない、複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記レジスタから取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【００６３】（３）　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記暗号処理用演算ユニットは、暗号化処理又は復号化処理のための演算動作と並行して次に演算の使用するデータを記憶回路から取り込む信号経路を設けることにより、演算動作とデータ転送とを同時に行なうようにすることができ、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【００６４】（４）　上記に加えて、上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2\ mod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2$ ｍｏｄＮの演算を行ない、かかる演算と並行して複数ビットの組み合わせに対応したＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【００６５】（５）　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理

用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記記憶回路から暗号処理用演算ユニットに供給される暗号化処理又は復号化処理のためのデータは、上記記憶回路に内蔵されたアドレス発生回路に上記中央処理装置から供給された先頭アドレスを基に形成されたアドレス信号に基づいて上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに乱数発生回路で形成された乱数を偽アドレス信号として送出することにより、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【００６６】（６）　上記に加えて、上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、上記複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【００６７】（７）　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記乱数発生回路で形成された乱数を用いて上記中央処理装置において形成された暗号化されたアドレス信号を上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成して暗号化処理又は復号化処理のためのデータを読み出して上記暗号処理用演算ユニットに転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、記憶回路に送られるアドレス信号の解読を困難にしつつ、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【００６８】（８）　上記に加えて、上記暗号化処理又は復号化処理は、ＲＳＡ暗号法などに応用可能なべき乗剰余乗算動作を含み、上記暗号化処理用演算ユニットは、入力されたＸ、Ｙ及びＮを受け、Ａ＝１、Ｂ＝Ｘとして、$A=A^2 \bmod N$とＡ＝ＡＢｍｏｄＮの演算を交互に行ない、かかる演算においてＹの上位から複数ビットずつみて、上記複数ビットに対応した$A=A^2 \bmod N$の演算を行ない、上記複数ビットの組み合わせに対応してＡＢｍｏｄＮの演算に必要なＢの値を上記記憶回路から取り込むことにより、暗号処理の高速化と機密保護とを実現できるという効果が得られる。

【００６９】（９）　中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納することにより、演算動作の過程でのデータ転送を無くすことができるから、電流波形を利用したアタックを無力化することができるという効果が得られる。

【００７０】（１０）　上記に加えて、上記各回路を１つの半導体基板上において形成することにより、モジュールの小型化を図りつつ、機密保護の強化を実現することができるという効果が得られる。

【００７１】（１１）　中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに暗号化処理又は復号化処理のための演算動作と並行して次の演算に使用するデータを記憶回路から取り込む信号経路を設けることにより、演算動作とデータ転送とを同時に行なうようにすることができ、レジスタの簡素化を図りつつ電流波形を利用したアタックを無力化することができるという効果が得られる。

【００７２】（１２）　中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、中央処理装置により暗号化処理又は復号化処理のためのデータの先頭アドレスを上記記憶回路に供給し、記憶回路では内蔵されたアドレス発生回路により形成されたアドレス信号によりデータを読み出して上記暗号処理用演算ユニットにデータ転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスに乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、回路の簡素化

を図りつつ、電流波形を利用したアタックを無力化することができるという効果が得られる。

【００７３】（１３）　中央処理装置、記憶回路、暗号処理用演算ユニット及び乱数発生回路とが共通のアドレスバスに接続され、上記中央処理装置からの指示を受けて動作する暗号処理用演算ユニットと記憶回路による暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記中央処理装置により上記乱数発生回路で形成された乱数を用いて暗号化処理又は復号化処理のためのデータの先頭アドレスを暗号化して上記記憶回路に供給し、記憶回路では上記乱数を用いて上記アドレス信号を復号化して先頭アドレスを生成し、それを基に形成されたアドレス信号に基づいてデータを読み出して上記暗号処理用演算ユニットに転送し、かかるデータ転送に対応して、上記中央処理装置、記憶回路及び暗号処理用演算ユニットが共通に接続されてなるアドレスバスには乱数発生回路で形成された乱数が偽アドレス信号として送出することにより、記憶回路に送られるアドレス信号の解読を困難にしつつ、偽アドレス信号により転送されるデータの電流波形を攪乱させることができるから、回路の簡素化を図りつつ、電流波形を利用したアタックを無力化することができるという効果が得られる。

【００７４】以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、ＩＣカードには、１つの半導体集積回路装置を搭載するもの他、複数の半導体集積回路装置が搭載されるものであってもよい。マイクロコンピュータは、１つの半導体集積回路装置に形成されるもの他、ＣＰＵとその周辺回路が複数チップで構成されて、１つのモジュール基板に搭載されてなるものであってもよい。

【００７５】演算処理は前記のような暗号処理を行なうべき乗剰余乗算法の他に、図２５図に示したフロチャート図のように演算Ａと演算Ｂを持ち、演算Ａの結果により演算Ｂを行なうか否かの分岐を持つような演算処理に広く利用することができる。つまり、演算Ａの次に演算Ｂを実行し、演算Ａの結果から演算Ｂが不要なら、その演算結果を無効にするような演算処理を行なえば、前記のような暗号処理以外の機密動作を必要とするデータ処理のハッキング対策として有益なものとなる。

【００７６】上記マイクロコンピュータは、データ処理装置とかかるデータ処理装置によるデータ処理手順が書き込まれたＲＯＭを含んで記データ処理手順に従ってデータの入出力動作が行われるものであれば何であってもよい。例えば、前記のようなＩＣカード用チップの他に、ゲーム用等の１チップマイクロコンピュータ等のように機密保護の必要な各種マイクロコンピュータに広く適用できるものである。この発明は、機密保護を必要とする各種ＩＣカード及びマイクロコンピュータに広く利用できる。

【００７７】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。すなわち、外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータをかかるレジスタに取り込むようにすることにより、演算動作の過程でのデータ転送を無くすことができるから、電流波形を利用したアタックを無力化することができる。

【００７８】中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むモジュール構成のマイクロコンピュータにおいて、上記暗号処理用演算ユニットに複数ビット単位での暗号化処理又は復号化処理のための演算に使用するデータを格納するレジスタを設け、暗号化処理又は復号化処理に先立って必要なデータを上記レジスタに格納することにより、演算動作の過程でのデータ転送を無くすことができるから、電流波形を利用したアタックを無力化することができる。

【図面の簡単な説明】

【図１】この発明が適用されるＩＣカードの一実施例を示す外観図である。

【図２】この発明に係るＩＣカードに搭載されるＩＣカード用チップの一実施例を示す概略ブロック図である。

【図３】この発明に係るコプロセッサの一実施例の動作を説明するためのタイミング図である。

【図４】図３のコプロセッサの動作を説明するためのフローチャート図である。

【図５】図３のコプロセッサの一実施例を示すブロック図である。

【図６】図３のコプロセッサの他の一実施例を示すブロック図である。

【図７】図３に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。

【図８】図３のコプロセッサの他の一実施例を示すブロック図である。

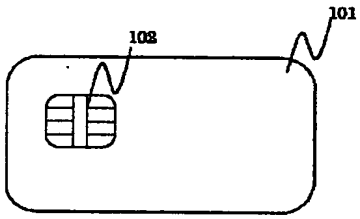
【図９】この発明に係るコプロセッサの他の一実施例の動作を説明するための構成図である。

【図１０】図９に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。

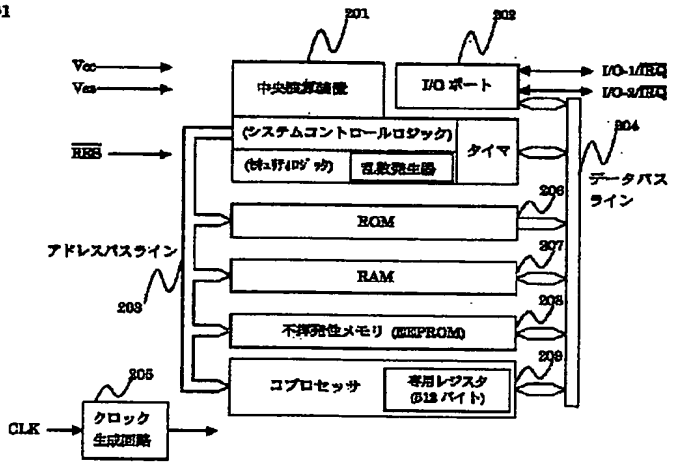
【図１１】この発明に係るコプロセッサの他の一実施例の動作を説明するためのタイミング図である。

【図１２】この発明に係るコプロセッサの他の一実施例の動作を説明するためのフローチャート図である。
【図１３】この発明に係るコプロセッサの他の一実施例の動作の詳細を説明するためのタイミング図である。
【図１４】図１１ないし図１３に示したコプロセッサの動作を実現するための一実施例を示すブロック図である。
【図１５】この発明に係るコプロセッサの更に他の一実施例の動作を説明するためのタイミング図である。
【図１６】この発明に係るコプロセッサの演算動作の他の一実施例を示すフローチャート図である。
【図１７】この発明に係るコプロセッサの他の一実施例を示すブロック図である。
【図１８】この発明に係るコプロセッサの他の一実施例を示すブロック図である。
【図１９】この発明に係るコプロセッサの他の一実施例を示すブロック図である。
【図２０】この発明に係るＩＣカード用チップの他の一＊実施例を示す要部ブロック図である。
【図２１】図２０のカウンタの一実施例を示すブロック図である。
【図２２】図２０のＩＣカード用チップの動作の一例を示すタイミング図である。
【図２３】この発明に係るＩＣカード用チップの更に他の一実施例を示す要部ブロック図である。
【図２４】図２３のＩＣカード用チップの動作の一例を示すタイミング図である。
【図２５】この発明が適用可能な演算動作を説明するためのフローチャート図である。
【符号の説明】
２０１…中央処理装置（ＣＰＵ）、２０２…Ｉ／Ｏポート、２０３…アドレスバス、２０４…データバス、２０５…クロック生成回路、２０６…ＲＯＭ、２０７…ＲＡＭ、２０８…ＥＥＰＲＯＭ、２０９…コプロセッサ（暗号化処理用演算ユニット）、ＣＤＡ、ＣＤＢ、ＣＤＮ、ＣＤＷ…レジスタ。

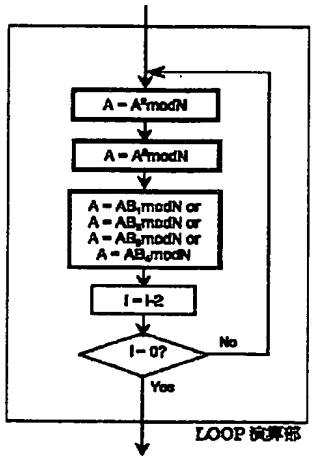
【図１】



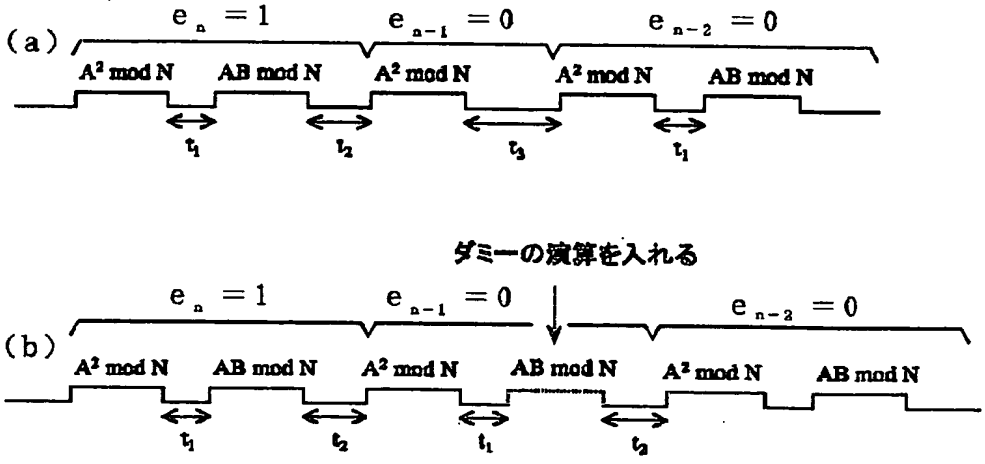
【図２】



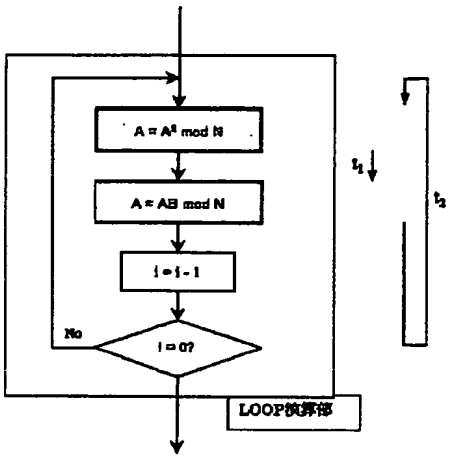
【図１６】



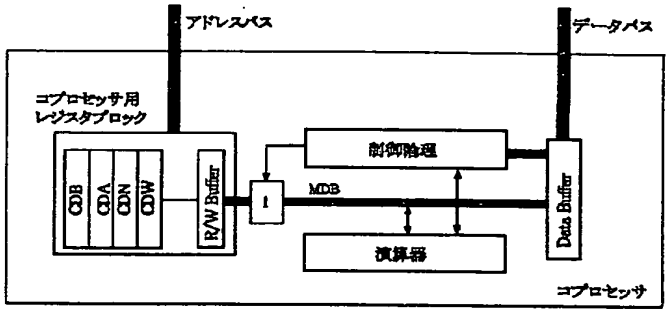
【図３】



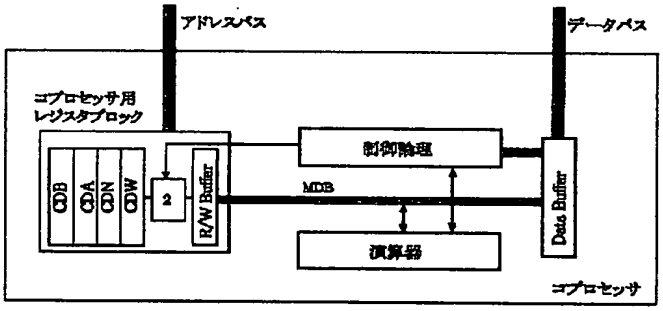
【図４】



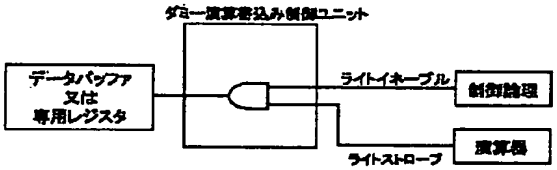
【図５】



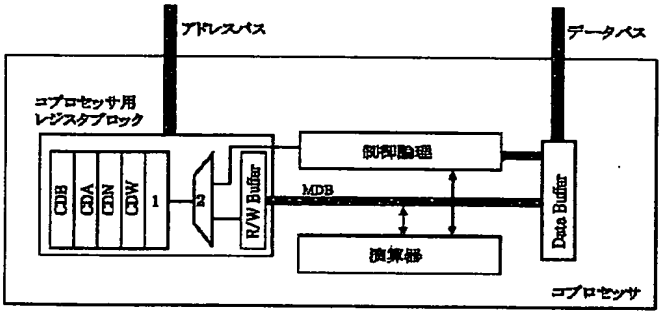
【図６】



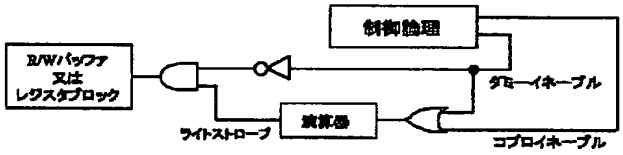
【図７】



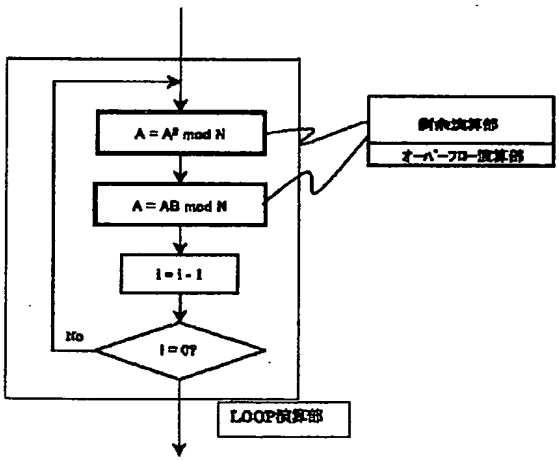
【図８】



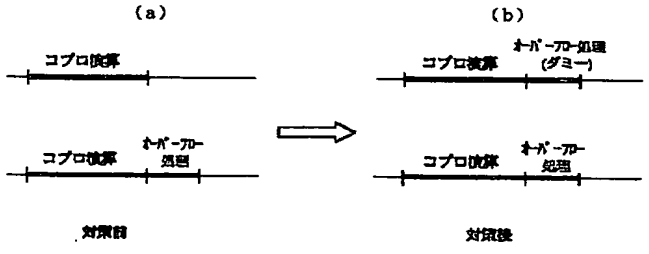
【図１０】



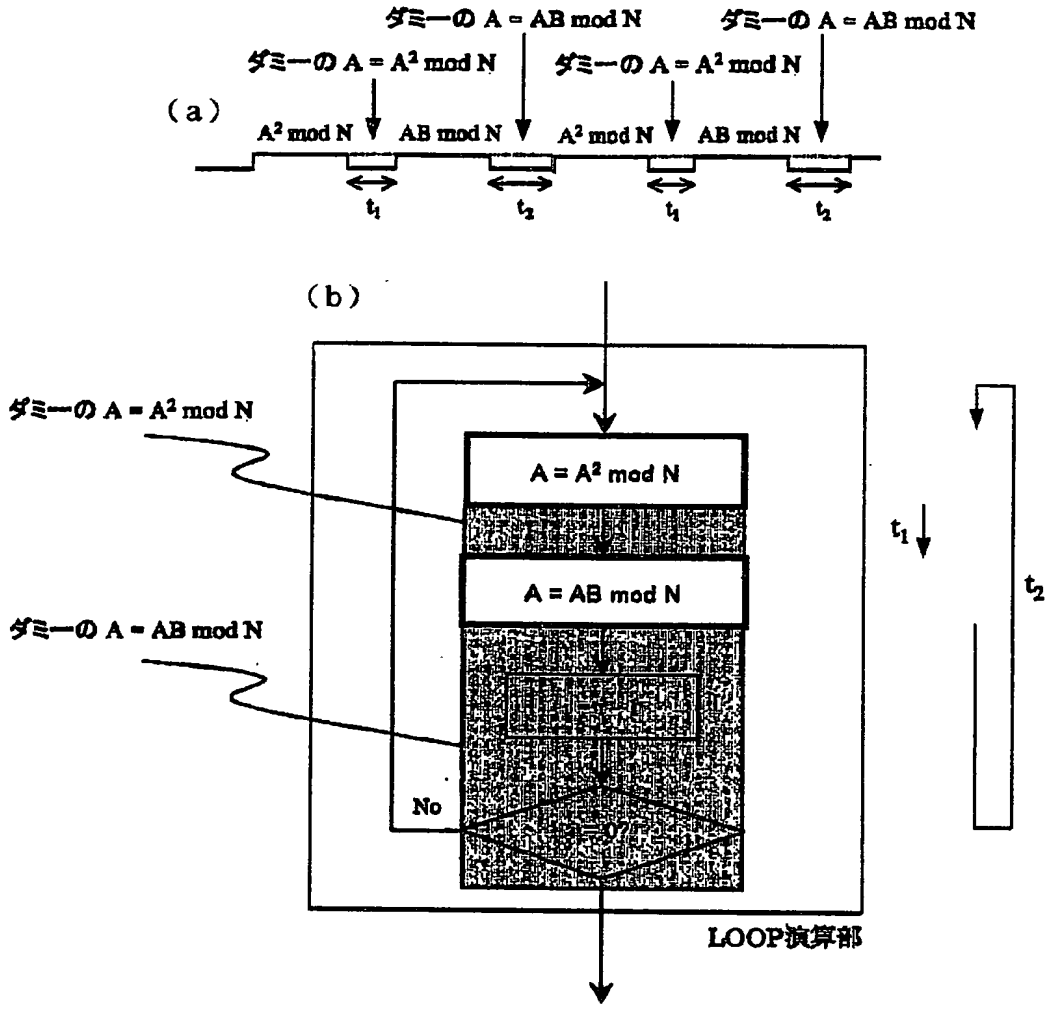
【図１２】



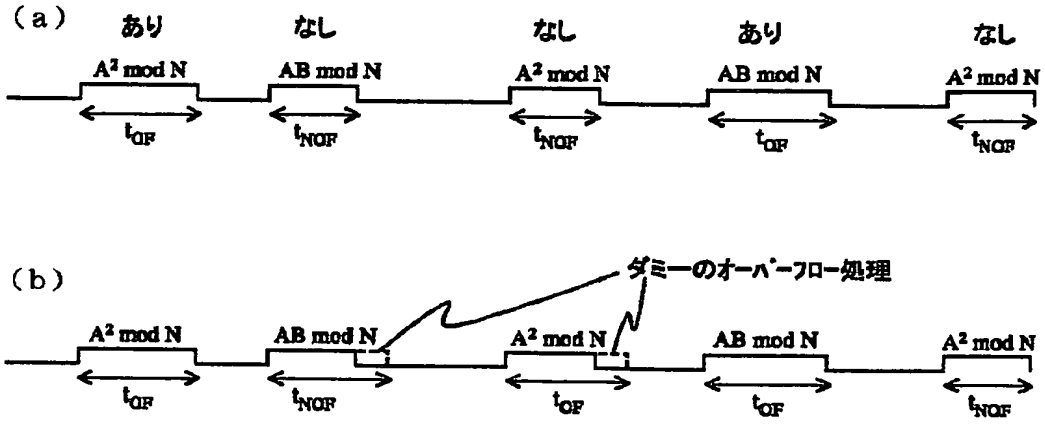
【図１３】



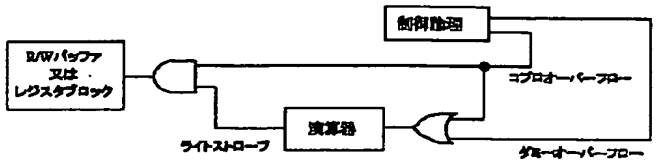
【図９】


ダミーの A = AB mod N
ダミーの A = AB mod N
ダミーの A = A² mod N
ダミーの A = A² mod N
(a)
A² mod N
AB mod N
A² mod N
AB mod N
t1
t2
t1
t2
(b)
ダミーの A = A² mod N
A = A² mod N
A = AB mod N
ダミーの A = AB mod N
No
LOOP演算部
t1
t2

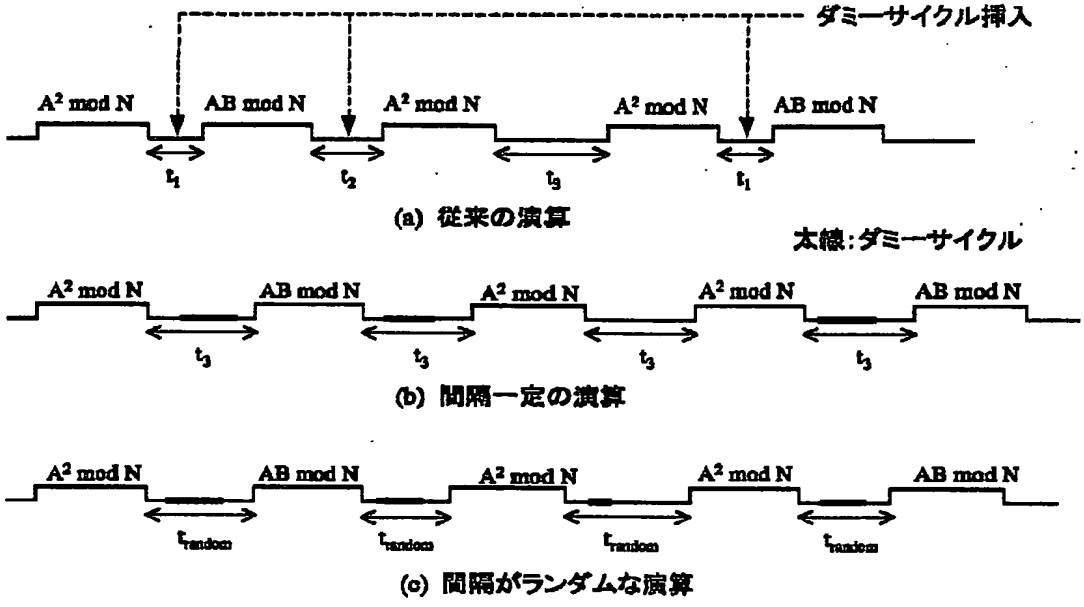
【図１１】


(a)
あり
なし
なし
あり
なし
A² mod N
AB mod N
A² mod N
AB mod N
A² mod N
tOF
tNOF
tNOF
tOF
tNOF
(b)
ダミーのオーバーフロー処理
A² mod N
AB mod N
A² mod N
AB mod N
A² mod N
tOF
tNOF
tOF
tOF
tNOF

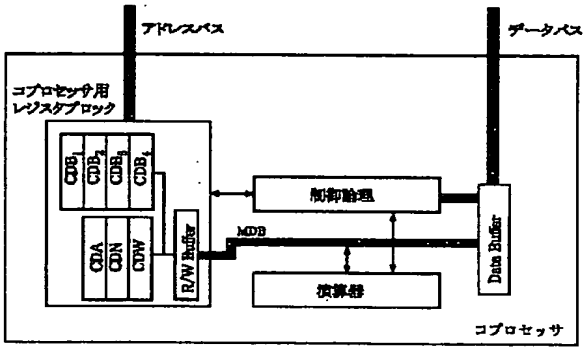
【図１４】



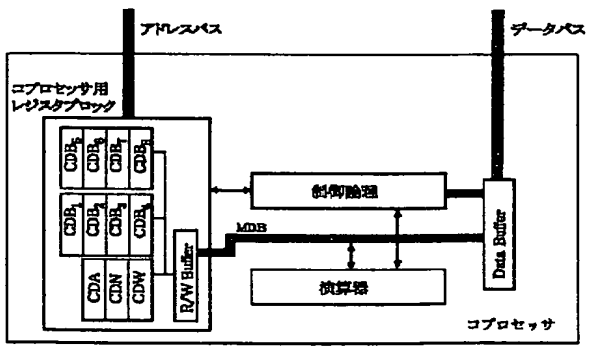
【図１５】



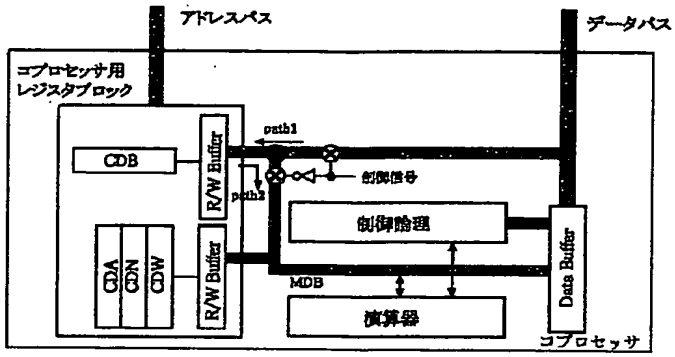
【図１７】



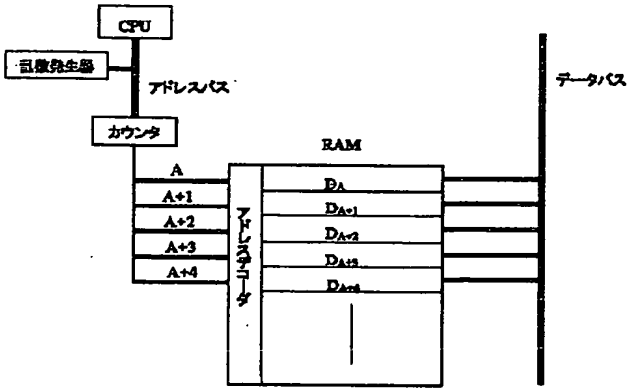
【図１８】



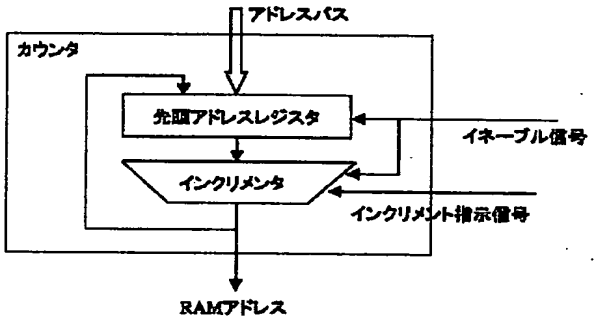
【図１９】



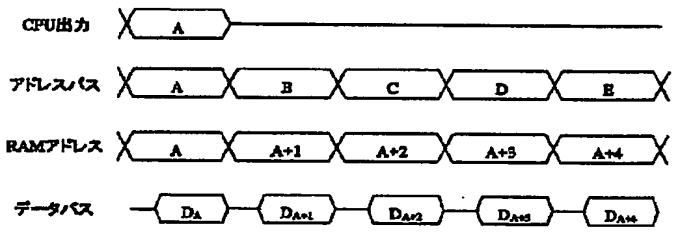
【図２０】



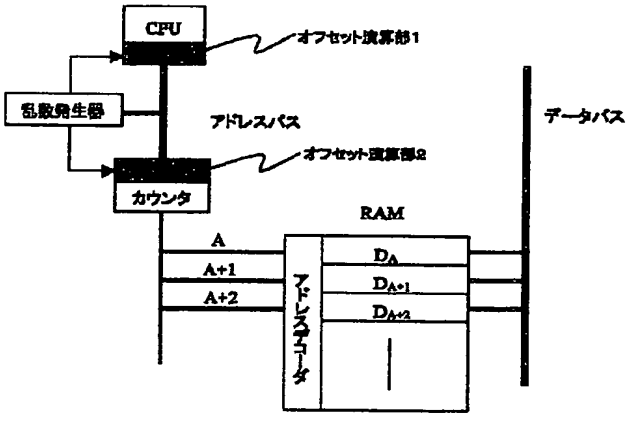
【図２１】



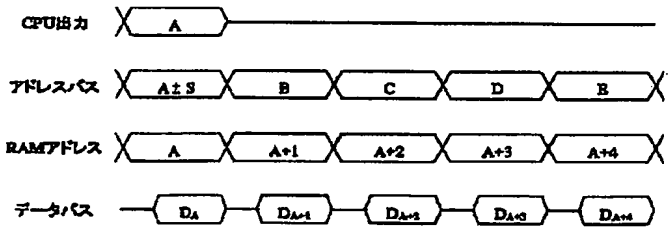
【図２２】



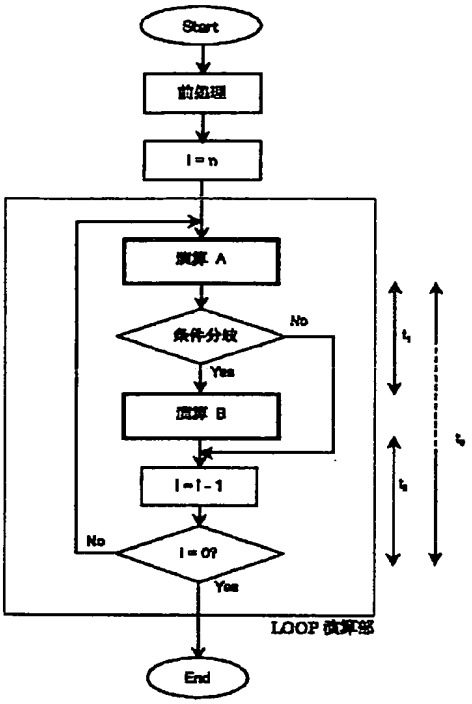
【図２３】



【図２４】



【図２５】



フロントページの続き

(72)発明者　中田　邦彦
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(72)発明者　塚元　卓
東京都小平市上水本町５丁目22番１号　日立超エル・エス・アイ・システムズ内
(72)発明者　渡瀬　弘
東京都小平市上水本町５丁目22番１号　日立超エル・エス・アイ・システムズ内

Ｆターム(参考)　5B017 AA03 BA07 BB09 CA14
5B035 AA13 BB09 CA38
5J104 AA41 JA28 NA02 NA18 NA22 NA35 NA40
9A001 EE03 JJ08 LL01